Google Inc. et al v. Egger et al

Doc. 272 Att. 1

EXHIBIT 2

Dockets.Justia.com

99TH CONGRESS 2d Session | HOUSE OF REPRESENTATIVES | REPORT 99-647

ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

JUNE 19, 1986.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. KASTENMEIER, from the Committee on the Judiciary, submitted the following

REPORT

[To accompany H.R. 4952]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 4952) to amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Electronic Communications Privacy Act of 1986".

TITLE I—INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS

SEC. 101. FEDERAL PENALTIES FOR THE INTERCEPTION OF COMMUNICATIONS.

(a) DEFINITIONS.—(1) Section 2510(1) of title 18, United States Code, is amended—

(A) by striking out "any communication" and inserting "any aural transfer" in lieu thereof;

(B) by inserting "(including the use of such connection in a switching station)" after "reception".

(C) by striking out "as a common carrier" and

(D) by inserting before the semicolon at the end the following: "or communications affecting interstate or foreign commerce, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit".

(2) Section 2510(2) of title 18, United States Code, is amended by inserting before the semicolon at the end the following: ", but such term does not include any electronic communication".

(3) Section 2510(4) of title 18, United States Code, is amended—

(A) by inserting "or other" after "aural"; and

"(4) the term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted, with respect to wire communications, on the telephone line to which such device is attached, but such term does not include any device used by a provider of wire communication service for billing, or recording as an incident to billing, for communications services provided by such provider; and

"(5) the term 'attorney for the Government' has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

"(6) the term 'State' means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.".

(b) CLERICAL AMENDMENT.—The table of chapters for part II of title 18 of the United States Code is amended by inserting after the item relating to chapter 205 the following new item:

"206. Pen Registers .... 3121".

SEC. 302. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b), this title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) SPECIAL RULE FOR STATE AUTHORIZATIONS OF INTERCEPTIONS.—Any pen register order or installation which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such order or installation occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of changes in State law required in order to make orders or installations under Federal law as amended by this title; or

(2) the date two years after the date of the enactment of this Act.

PURPOSE

The purpose of the legislation is to amend title 18 of the United States Code to prohibit the interception of certain electronic communications; to provide procedures for interception of electronic communications by federal law enforcement officers; to provide procedures for access to communications records by federal law enforcement officers; to provide procedures for federal law enforcement access to electronically stored communications; and to ease certain procedural requirements for interception of wire communications by federal law enforcement officers.

HISTORY

When the Framers of the Constitution acted to guard against the arbitrary use of government power to maintain surveillance over citizens, there were limited methods of intrusion into the "houses, papers and effects" protected by the Fourth Amendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions.

The telephone is the most obvious example. Its widespread use made it technologically possible to intercept the communications of citizens without entering homes or other private places. When the issue of government wiretapping first came before the Supreme Court in *Olmstead* v. *United States,* 277 U.S. 438, the Court held that wiretapping did not violate the Fourth Amendment, since there was no searching, no seizure of anything tangible, and no physical trespass.[1]

But the *Olmstead* case is remembered not only for its holding but for the prescient dissent of Mr. Justice Brandeis, who predicted:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home . . . Can it be that the Constitution affords no protection against such invasions of individual security?[2]

Forty years later, the Supreme Court accepted the logic of Justice Brandeis in *Katz* v. *United States,* 389 U.S. 347 (1967), holding that the Fourth Amendment applies to government interception of a telephone conversation. At the same time, the Court extended Fourth Amendment protection to electronic eavesdropping on oral conversations in *Berger* v. *New York,* 388 U.S. 41 (1967).

Congress responded in a comprehensive fashion by authorizing government interception, under carefully subscribed circumstances, in Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[3] which has come to be known as the Wiretap Act. That legislation protected two common types of communication—telephone conversations and face-to-face oral communications—against electronic eavesdropping. Specifically, the law barred the interception of wire communications over a common carrier unless an appropriate court order had been obtained.[4] Further, it limited the concept of interception to the "aural acquisition" of the contents of a communication.[5] "Oral communications" were protected only in circumstances where there is a reasonable expectation of privacy.[6]

NATURE OF THE PROBLEM

Although it is still not twenty years old, the Wiretap Act was written in different technological and regulatory era. Communications were almost exclusively in the form of transmission of the human voice over common carrier networks. Moreover, the contents of a traditional telephone call disappeared once the words transmitted were spoken and there were no records kept. Consequently the law primarily protects against the aural interception of the human voice over common carrier networks.

The legislation did not attempt to address the interception of text, digital or machine communication.[7] This statutory framework appears to leave unprotected an important sector of the new communications technologies.

Many communications today are carried on or through systems which are not common carriers. Electronic mail, videotex and similar services are not common carrier services. Under existing law the interception of these services or the disclosure of the contents of messages over these services are probably not regulated or restricted. Moreover, totally private systems are rapidly being developed by private companies for their own use. It is not uncommon for businesses now not to use the local telephone comapny in some instances the long distance companies in the creation of voice and data networks. Since these networks are private they are not covered by existing Federal law. In addition, data is transmitted over tradional telephone services as well as by these services. Since data, unlike the human voice, cannot be aurally intercepted, it is also largely unregulated and unrestricted under present law.

---

[1] Olmstead v. United States, 277 U.S. 438, 464 (1927). *Compare,* Dow Chemical Co. v. United States, — U.S. — (May 19, 1986) (aerial photography by government without a warrant does not violate Fourth Amendment); California v. Ciraolo, — U.S. — (May 19, 1986) (same).

[2] 277 U.S. at 474 (Brandeis, J., dissenting).

[3] 18 U.S.C. 2510 *et seq.* hereinafter "Wiretap Act."

[4] 18 U.S.C. 2511.

[5] 18 U.S.C. 2510.

[6] *Id.*

[7] Sen. Rep. No. 1097, 90th Cong., 2d Sess. 90, hereinafter "1968 Senate Report."

Today, we have large-scale electronic mail operations, cellular and cordless telephones, paging devices, miniaturized transmitters for radio surveillance, and a dazzling array of digitized information networks which were little more than concepts two decades ago. Unfortunately, the same technologies that hold such promise for the future also enhance the risk that our communications will be intercepted by either private parties or the government.

In 1984 the Federal government engaged in more telephone surveillance and wiretapping than in any year since 1973.[8] Moreover, according to a recent study by the Office of Technology Assessment, Federal agencies are planning to use or already use radio scanners (20 agencies), cellular telephone interception (6 agencies), tracking devices (15 agencies), pen registers (14 agencies), and electronic mail interceptions (6 agencies).[9]

This increased use of a variety of electronic surveillance devices alone is not cause for alarm. There are instances when a particular electronic surveillance technique is justified in a criminal investigation. Congress has recognized this by permitting—under carefully limited circumstance under the Wiretap Act—the tapping of telephone calls or the bugging of rooms. However, despite efforts by both Congress [10] and the courts,[11] legal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology.

The statutory deficiency in Title III with respect to non-voice communications has been criticized by commentators, Congressional experts, and most recently by both the General Accounting Office and the Office of Technology Assessment.[12] The danger is eloquently pointed out by Professor Richard Posner (now United States Circuit Court Judge):

[8] Administrative Office of the United States Courts, *Report on Application for Orders Authorizing or Approving the Interception of Wire or Oral Communications (Wiretap Report) for the Period January 1, 1984 to December 31, 1984.*

[9] Office of Technology Assessment, U.S. Cong., ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES (1985), hereinafter "OTA Report."

[10] *E.g.*, The Wiretap Act, *supra* note 3; Foreign Intelligence Surveillance Act, 50 U.S.C. 101 *et seq.*; Right to Financial Privacy Act, 12 U.S.C. 3401 *et seq.*

[11] *E.g.*, United States v. Torres, 751 F.2d 875 (7th Cir. 1984), *cert. den'd.* —U.S.—, 105 S.Ct. 1853 (1985). (court has authority to issue warrant permitting video surveillance); Katz v. United States, 389 U.S., 347 (1967), (Fourth Amendment applies to government wiretapping of telephone conversation); Berger v. New York, 388 U.S. 41 (1967) (Fourth Amendment applies to electronic eavesdropping on oral conversation).

[12] *See generally, Electronic Communications Privacy Act of 1985: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the House Comm. on the Judiciary*, 99th Cong., 1st and 2d Sess., hereinafter "House Hearings." *See also* Burnham, *Experts Study Effect on Law of Latest Electronic Services*, N.Y. Times, Mar. 18, 1985 (reporting on study by ACLU Project on Privacy and Technology).

In the absence of market discipline, there is no presumption that the government will strike an appropriate balance between disclosure and confidentiality. And the enormous power of the government makes the potential consequences of its snooping far more ominous than those of . . . a private individual or firm.[13]

This legal uncertainty poses potential problems in a number of areas. First, it may unnecessarily discourage potential customers form using such systems, and encourage unauthorized users to obtain access to communications to which they are not party.[14] Lack of clear standards may also expose law enforcement officers to liability [15] and endanger the admissibility of evidence.[16]

But most important, if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right.[17] Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.[18] Additional legal protection is necessary to ensure the continued vitality of the Fourth Amendment.[19]

The Committee believes the bill represents a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement.

TELECOMMUNICATIONS TECHNOLOGIES UNDER CURRENT LAW

RADIO TELEPHONES

When Congress passed the Wiretap Act in 1968, most telephone calls were transmitted as they always had been—by wire. Other technologies, however, were already on the horizon, an inevitability implicitly recognized by Congress in protecting telephone calls carried "in whole or in part" over wire. 18 U.S.C. 2510. Today, only a minority of telephone calls are made through wire alone; the majority combine wire with some form of radio technology, usually microwave.

a. Microwave

Microwave consists of extremely high frequency radio waves transmitted point-to-point on line-of-sight paths between antennas located on towers or building tops (in terrestrial microwave systems) and between satellites and earth station "dish" antennas (in satellite-based systems). Like most radio transmissions, the microwave portion of a telephone call is vulnerable to interception.[20]

[13] Posner, *Privacy in the Supreme Court*, 1979 Sup. Ct. Rev. 173, 176 (1979).

[14] House hearings, *supra* note 12 (testimony of P. Walker, P. Quigley, P. Nugent, J. Stanton *et al.*)

[15] *See* Malley v. Briggs, —U.S.— (84-1586, Mar. 5, 1986), 54 U.S.L.W. 4243 (Mar. 5, 1986).

[16] 18 U.S.C. 2515.

[17] According to a recent poll, 77 percent of Americans are concerned about technology's threats to their personal privacy. Louis Harris & Associates, *The Road After 1984*, Southern New England Telephone (1984).

[18] *See* Dow Chemical v. United States, —— US. —— (May 19, 1984) (Powell, J. dissenting).

[19] For recent explorations on the capacity of Congress to interpret the Constitution, *see* Mikva, *How Well Does Congress Support and Defend the Constitution?*, 61 N.C. L. Rev. 587 (1983); Fisher, *Constitutional Interpretation by Members of Congress*, 63 N.C. L. Rev. 707 (1985).

[20] T. Harrington and B. Cooper, THE HIDDEN SIGNALS ON SATELLITE TV (1984).